

Remarks

Claims 1-6, 8-9, and 20-40 are in the application. Claims 7 and 10-19 have been cancelled. Claims 1, 20, 27 and 33 are in independent form. Reconsideration is requested.

The Examiner notes the claim to priority from provisional application no. 60/462,080 filed April 11, 2003, but that reference to the provisional application is not included in the application text. The application has been amended to recite the claim for priority, and a petition for an unintentionally delayed benefit claim under 35 USC 119(e). Applicant notes that the entire delay between the date the claim was due and the date the claim was filed was unintentional.

The specification is objected to as requiring a statement of the status of all parent priority applications. Applicant notes that priority is claimed only from a provisional application. Priority is not claimed for any standard application. Applicant requests, therefore, that this objection be withdrawn.

Claims 1 and 17 are objected to for typographical informalities. Amended claim 1 corrects the informality identified by the Examiner, and claim 17 has been cancelled. Applicant requests that this objection be withdrawn.

1, 2, 5-11, 13, 16-18 stand rejected under 35 USC 102(b) for anticipation by US Publication No. 2003/0046447 by Kouperchaliak (hereafter Kouperchaliak). Claims 3-4, 12, 14-15 and 19 stand rejected under 35 USC 103(a) as being unpatentable over Kouperchaliak in view of Publication No. 2002/0145643 to Shmueli et al. (hereafter, Shmueli). Applicant responds as follows.

Kouperchaliak is directed to providing improved "plug & play" functionality of USB computer peripherals by allowing a USB peripheral to install the drivers needed to operate with a host computer. For example, Kouperchaliak describes a printer that has stored on it "device-related software (DRS)" (e.g., software drivers) that permit interaction between the printer and the computer. The printer checks whether device-related software (i.e., drivers) are already installed on the

host computer and, if not, uploads the device-related software to the computer for the proper installation and operation of the peripheral device by the computer.

Shmueli describes a portable memory device or “key” that runs an authentication routine to ensure that the holder of the key is authorized to use it on a host computer. The authentication routine provides a user authentication interface that requires a password, logon information, or biometric indicia from a biometric reader associated with the host 12. The user provides the authentication indicia to the host and the authentication routine, which is running on the host, determines if the user is authenticated and provides access to data on the key accordingly.

Amended claim 1 recites an integrated circuit flash drive memory device that is connectable to a host computing device and includes a memory component storing an arbitrary application software operable on the host computing device. Autorun software stored on the integrated circuit memory device to installs the arbitrary application software on the host computing device automatically upon activation of the integrated circuit memory device with the host computing device. The use of the integrated circuit flash drive memory device for installation of arbitrary software is described throughout the application, such as at application paragraph numbers [002]-[006] and [045]. Applicant submits that amended claim 1 is patentably distinct from the cited references for the following reasons.

Kouperchaliak is directed to providing improved “plug & play” functionality of USB computer peripherals by allowing a USB peripheral to install the drivers needed to operate with a host computer. Kouperchaliak provides no teaching or suggestion of using the described USB computer peripherals to install arbitrary software. Moreover, being directed to the installation of device drivers directly from associated USB peripheral devices, Kouperchaliak provides no teaching or suggestion of incorporating the described manner of installing device drivers into the operation of an integrated circuit flash drive memory device, as recited in claim 1.

Rather, applicant submits that the focus of Kouperchaliak on the installation of device drivers would lead one skilled in the art away from using the installation technique in an integrated circuit flash drive memory device. Also, the authentication system of Shmueli for accessing data on a portable "key" provides no teaching or suggestion of the subject matter of claim 1. Applicant submits, therefore, that claim 1 is patentably distinct from the cited references and requests that the rejection be withdrawn.

Applicant submits that claims 2-6 and 8-9 are allowable as dependents of claim 1 and are further allowable for the following reasons.

Amended claim 3 recites that the integrated circuit flash drive memory device of claim 1 includes a protected memory component and that selected software is stored in the protected memory component and in which the selected software is accessible only by the autorun software upon authentication of the autorun software. Kouperchaliak provides no teaching or suggestion related to such a protected memory component. Shmueli describes an authentication system (e.g., password-protection) through which a user can access data stored on a portable "key." Applicant notes, however, that Shmueli provides no teaching or suggestion of an integrated circuit flash drive memory device with a protected memory component that is accessible only by authenticated autorun. Claim 3 provides no manner for a user to access the protected memory component. Applicant submits, therefore, that claim 3 is patentably distinct from the cited references and requests that the claim be allowed.

Amended claim 5 recites an integrated circuit flash drive memory device of with a user operable manual switch that allows a user to select from among plural operating states that include a first state in which the autorun software is operable and a second state in which the autorun software is not operable so that the integrated circuit flash drive memory device functions as a conventional integrated circuit flash drive memory device. Shmueli describes a portable "key" with an authentication system that does not relate to such a switch. Kouperchaliak includes a function switch that automatically switches a peripheral

device between a device driver installation mode and a normal peripheral function mode according to whether the device driver is installed on a host computer.

Kouperchaliak provides no teaching or suggestion related to a user-operable switch that allows user-selection of an operating mode. Rather than being mere design choice, the fully-automated operation of the "function switch" of Kouperchaliak relates directly to the one-time installation of device drivers. Applicant submits, therefore, that claim 5 is patentably distinct from the cited references.

New independent claim 20 is analogous to original claims 1 and 3 and recites an integrated circuit memory device having a memory component storing selected software operable on the host computing device and autorun software stored on the integrated circuit memory device to install the selected software on the host computing device automatically upon activation of the integrated circuit memory device with the host computing device. Claim 20 further recites that the memory component includes a protected memory component where the selected software is stored component so as not to be viewable and is accessible only by the autorun software during installation of the selected software, thereby providing copy protection of the selected software.

Kouperchaliak provides no teaching or suggestion related to such a protected memory component. Shmueli describes an authentication system (e.g., password-protection) through which a user can access data stored on a portable "key." Applicant notes, however, that Shmueli provides no teaching or suggestion of an integrated circuit memory device with a protected memory component where the selected software is stored component so as not to be viewable and is accessible only by the autorun software during installation of the selected software. Claim 20 provides no manner for a user to access the protected memory component, as described by Shmueli. Applicant submits, therefore, that claim 20 is patentably distinct from the cited references and requests that the claim be allowed.

New claims 21-26 depend from claim 20 and are analogous to corresponding ones of claims 2-6 and 8-9. Applicant submits that claims 21-26 are further allowable for the reasons set forth above with regard to claims 2-6 and 8-9.

New claim 27 is analogous to amended claim 1 and further recites a user operable manual switch that allows a user to select from among plural operating states that include a first state in which the autorun software is operable and a second state in which the autorun software is not operable so that the integrated circuit flash drive memory device functions as a conventional integrated circuit flash drive memory device.

Shmueli describes a portable “key” with an authentication system that does not relate to such a switch. Kouperchaliak includes a function switch that automatically switches a peripheral device between a device driver installation mode and a normal peripheral function mode according to whether the device driver is installed on a host computer. Kouperchaliak provides no teaching or suggestion related to a user-operable switch that allows a user to select from among plural operating states that include a first state in which the autorun software is operable and a second state in which the autorun software is not operable so that the integrated circuit flash drive memory device functions as a conventional integrated circuit flash drive memory device. Rather than being mere design choice, the fully-automated operation of the “function switch” of Kouperchaliak relates directly to the one-time installation of device drivers. Applicant submits, therefore, that claim 27 is patentably distinct from the cited references.

New claims 28-32 depend from claim 27 and are analogous to corresponding ones of claims 2-6 and 8-9. Applicant submits that claims 28-32 are further allowable for the reasons set forth above with regard to claims 2-6 and 8-9.

New independent claim 33 recites an integrated circuit wireless device connectable to a host computing device and includes a wireless component for enabling the host computing device wireless connectivity with the wireless

component. A memory component included in the wireless integrated circuit device for storing wireless application software operable on the host computing device and autorun software stored on the integrated circuit wireless device to install or run the wireless application software on the host computing device automatically upon activation of the integrated circuit wireless device with the host computing device. New claim 33 further recites that the memory component includes a protected memory component where the wireless application software is stored so as not to be viewable and is accessible only by the autorun software during installation or running of the wireless application software, thereby providing copy protection of the wireless application software. Applicant submits that the new independent claim 33 is distinct from the cited references for reasons as follows.

Kouperchaliak provides no teaching or suggestion related to an integrated circuit wireless device connectable to a host computing device and includes a wireless component for enabling the host computing device wireless connectivity with the wireless component. Shmueli describes a portable “key”, and depicts in Fig 2C “a wireless communication device 10C, such as a transponder, capable of facilitating wireless communication with the host 12...”. Shumeli suggested that the “key”(device 10C) would communicate wireless with the host that is wireless enabled. To communicate wirelessly with the host, Shumeli suggested that the “key” (device 10C) “may incorporate an automatic detection or sensing technology, such as the discovery process used by Bluetooth” to communicate with a Bluetooth host. As such, the host must be Bluetooth enabled before it can discover or be discovered by the “key” that includes Bluetooth. Therefore, Shmueli did not teach or suggest a method of an integrated circuit wireless device connectable to a host computing device and includes a wireless component for enabling the host computing device wireless connectivity with the wireless component.

Analogous to claim 1, 3, and 20, neither Shmueli nor Kouperchaliak teaches or suggest a wireless device with a memory component storing wireless application software operable on the host computing device and autorun software

stored on the integrated circuit wireless device to install or run the wireless application software on the host computing device automatically upon activation of the integrated circuit wireless device with the host computing device.

Furthermore, analogous to claim 3, and 20, Kouperchaliak provides no teaching or suggestion related to protected memory component. Shmueli describes a user authentication system (e.g., password-protection) through which a user can access data stored on a portable "key." Shmueli provides no teaching or suggestion related to an integrated circuit device that includes a protected memory component where the wireless application software is stored so as not to be viewable and is accessible only by the autorun software during installation or running of the wireless application software, thereby providing copy protection of the wireless application software.

New dependent claims 34-37 are dependent of claim 33, and therefore it follows that the dependent claims 34-37 are also distinct and patentable.

Applicant believes the application is in condition for allowance and respectfully requests the same.

IPSONON LLP
111 SW COLUMBIA #710
PORTLAND, OREGON 97201
TEL. (503) 249-7066
FAX (503) 249-7068

Respectfully Submitted,


Mark M. Meininger
Registration No. 32,428